I hereby certify that this paper (12 pages) is being facsimile transmitted to the USPTO on the date shown below.
Date July 5 '05
Edward Langer, Reg. No. 30,564

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of : Redler, Yeshayahu

Serial No. : 09/786,364

Filed : March 15, 2001

For : SECURE DATA ENTRY PERIPHERAL DEVICE

Group Art Unit 2134
Examiner: SIMITOSKI, Michael J.

Tel Aviv, Israel
July 5, 2005

Hon. Commissioner of Patents and Trademarks
Alexandria, VA

REPLACEMENT FILING TO JULY 3, 2005 SUBMITTAL

Sir:

PETITION TO WITHDRAW FINAL REJECTION AS PREMATURE

PETITION UNDER 37 CFR SEC 1.181

Applicant hereby petitions to withdraw the Final Rejection status of the Office Action mailed April 5, 2005 as premature.

Applicant believes that the Final Rejection was mailed:
1) before the development of an issue, and
2) the Final Rejection contains a technical inaccuracy which reflects a misunderstanding on the part of the Examiner, resulting in a "hasty" and inconsistent prosecution record.

To support this position, Applicant presents his supporting arguments.

TIMING OF THIS PETITION

The present petition is being submitted after the May 31, 2005 telephone interview, conducted after receipt of the Final Rejection Office Action. The Final Rejection was mailed on April 5, 2005.

It is believed that in these circumstances, that this petition is timely, as the case is still pending per MPEP Sec. 706.07(d), and the telephone Interview summary generated on June 1, 2005 indicates that the Examiner is not inclined to accept any post final rejection amendment, since he believes that a new search is required.

SUMMARY OF PROSECUTION HISTORY

The subject application was filed on March 15, 2001 as a National Stage of a PCT application having an international filing date of September 16, 1999.

The first Office Action was mailed after a long delay of 3 and a half years, on September 21, 2004.

A response to the first Office Action was filed on December 21, 2004.

A Final Rejection Office Action was mailed on April 5, 2005 rejecting all of the claims.

In a post-final telephone interview with the Examiner, conducted by telephone on 31 May 2005, a proposed amendment was suggested to the independent claims relating to a public key algorithm.

In the Interview Summary mailed June 1, 2005, the Examiner indicated that if this amendment were submitted in an after-final amendment, an Advisory Action would be mailed indicating a need for further search and consideration.

The above summarizes the status of the prosecution thus far.

FINAL REJECTION SENT PRIOR TO DEVELOPMENT OF AN ISSUE - PLACES UNFAIR EXTRA BURDEN ON APPLICANT

In the discussion with the Examiner during the post-final telephone interview, the issue of a "secure keyboard device in a computer system adapted for Internet communication" was identified as the key to patentability, as the Examiner admitted that Clark ('569) does not disclose an environment related to Internet communication.

More specifically, the invention relates to a public key algorithm, and Clark does not.

Therefore, the Examiner's statement that an after final amendment on this point will require a further search is not acceptable.

The reason for this is that with respect to the present invention, there is a long prosecution history, including prior art references cited and arguments made, which placed the matter of an Internet communication context as a major, primary theme.

As proof of this, in the PCT prosecution of International Application PCT/IL 99/00504, a Written Opinion of the IPEA/US was mailed on October 2, 2000. After an interview with Examiner Rita Ziemer by the undersigned on November 21, 2000, it was indicated in the Interview Summary that the cited prior art could be overcome by an amendment.

Although the Clark ('569) reference used in the final rejection was not cited in the PCT prosecution, Applicant responded to the Written Opinion in a letter dated November 29, 2000 (a copy of which is attached here) by clearly stating that the invention was related to Internet E-commerce (see page 2, first line).

The context of the invention was originally framed in relation to the rise of the Internet data highway, which has dramatically increased the need for secure data transmission, per the background in the specification at page 1, 1st paragraph, lines 1 to 9.

From the above it is clear that the surrounding technology of the inventive method and device was always secure data transmission related to Internet communication. Not only was this stated in the original specification, but also, as part of the PCT examination process, **conducted by USPTO Examiners**, it was argued and highlighted by the Applicant that the invention was related to Internet communication.

Therefore, the Examiner's statement in the Interview Summary that he will require a new search is not acceptable.

Applicant believes that the Examiner should have taken the proper search context into account with his initial search.

TECHNICAL INACCURACY OF THE FINAL REJECTION

As understood by the Applicant's attorney, if there is a technical inaccuracy in the Final Rejection, this can be

considered as a basis for the present petition to withdraw the Final Rejection and re-open the prosecution.

It is believed that the Examiner has misunderstood the technical basis of the invention, which is to provide encryption and decryption techniques strong enough to meet the requirements of a secure Internet communication format.

The system described by the Clark patent ('569) largely relates to typical transactions within closed systems, e.g. ATM, banks, lottery, that employ encryption methods, such as a PIN code, as described in the background, per col. 1, lines 39-48. This is additionally stated in the description, at col. 2, lines 30-36 and at col. 8, lines 19-29.

However, encryption methods, such as a PIN code, may only provide a low security level within closed systems. Therefore, the encryption methods to which Clark relates are completely inadequate for encoding and decoding data information in a secure Internet communication format known today.

The technical inaccuracy of the final rejection is that it places encryption methods, such as the PIN code of Clark ('569), at the same security level as the public key algorithm disclosed in the present invention.

It is Applicant's position that the Examiner's statement in the telephone interview indicates a technical inaccuracy, since the Internet context, which is in common-use today, requires strong encryption and decryption techniques.

Therefore, it is concluded that the Examiner's statement that there is a need for a new search is unacceptable.

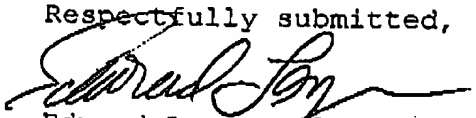
It should have been clear from the outset, in view of the PCT prosecution history, which was available to the Examiner, that the initial search should have been conducted in relation to the Internet context.

It is believed that the technical inaccuracy of the current Final Rejection is established, since the Internet context requires stronger encryption and decryption techniques. The Examiner should have understood this as a technical distinction as he began organizing his searching efforts.

Therefore, it remains Applicant's position that the finality of the last Office Action was premature, and the status of the application should be changed so that it is not in the post-final rejection condition.

Therefore, it is respectfully requested that the present petition be reviewed promptly and that the Applicant be notified of any questions requiring an immediate response, with a view toward resolving the status of this case immediately.

Respectfully submitted,



Edward Langer, Pat. Atty.
Attorney for Applicant
Reg. No. 30, 564

Shiboleth, Yisraeli, Roberts and Zisman LLP
350 Fifth Ave., 60th Floor
New York, NY 10118
212-244-4111 telephone
212-563-7108 fax

324191/1

EDWARD LANGER, B.S.E.E., M.B.A., J.D.
ADVOCATE & PATENT ATTORNEY

312 GIRON CENTER. P.O.B. 410 RAANANA 43103 ISRAEL
TEL: 972-9-7713585 FAX: 972-9-7713593 E-MAIL: edlanger@netvision.net.il

29 November, 2000
1063rsp.doc

Hon. Commissioner of Patents and Trademarks
BOX PCT
Washington, D.C. 20231
Attn: Rita Ziemer, Examiner

Re: International Application No. PCT/IL99/00504
Applicant: Yeshayahu Redler
Title: "SECURE DATA ENTRY PERIPHERAL DEVICE"
Our File : 1063

RESPONSE TO WRITTEN OPINION

Dear Sir,

In response to the Written Opinion of the IPEA/US mailed October 2, 2000, and in light of the interview conducted with Examiner Rita Ziemer by the undersigned, on November 21, 2000, please find enclosed herewith amended pages and claims for the above-referenced International Application. Pages 20, 21, and 22 have been amended, and page 23 has been deleted. Claims 1 and 22 have been amended. Claims 2-11, 16-21 and 23-24 have been deleted. The enclosed pages 20-22 are intended to replace pages 20-23 of the application.

REMARKS

It is the object of the present invention to provide a secure keyboard with a non-volatile storage memory associated with a controller chip. The "regular" keyboard controller chip is replaced by a chip with a non volatile memory, which provides a secure environment for credit card information, user access codes , ID information, etc. When the keyboard is used to conduct Internet transactions, the credit card etc. information is encrypted inside the keyboard and then sent via the PC to the Internet.

The advantages of the inventive secure keyboard include the fact that it is a "self-contained" solution.

Hon. Commissioner of Patents and Trademarks
BOX PCT
Washington, D.C. 20231

The Internet E-commerce has forced the design of hardware and software with special security provisions. Typically, the PC environment has solved this requirement by using the "add-on" approach , but when it comes to security, this is problematic. The approach has always been that the security is provided by the issuer of the credit card information, using removable media, that is, removably insertable media such as smartcards. The card issuer is thus like "Big-Brother" since it has access to secret data placed on the smartcard, and this data is not accessible to the user, nor is the user aware of its existence. The card issuer must then also "support" the smartcard and its hardware such as readers etc.

By contrast, the inventive solution provides a self-contained, easy-to-install device which is the keyboard itself, modified so as to contain a chip capable of encryption/decryption and data storage. The data is entered via the keyboard and the keyboard does not use predetermined data or hidden data.

As amended, claims 1 and 22 incorporate the recitation of claims 10, 11 regarding the secure keyboard configuration.

The Examiner has rejected claims 1-22 for lack of novelty and inventive step.

The prior art cited to Hughes suggests a smart card reader/interface, and this uses removable media. The card issuer (or authority) exists "outside" of the system.

The prior art Angelo patent does not suggest a secure keyboard, rather a secure system, which can easily be bypassed by modern "Trojan horse" penetration techniques into the computer.

The inventive approach of having the keyboard serve as a stand alone security device is novel, since at the time of Hughes and Angelo it was assumed that there is a need to protect only information that is distributed by a third party, such as a bank, credit card company, etc. It was also assumed that these

Hon. Commissioner of Patents and Trademarks
BOX PCT
Washington, D.C. 20231

third parties would distribute this information through physical devices (such as smartcards and credit cards). With the evolution of the Internet, many on-line services have been created that require the user to input a password. This method is used because it is simple and cheap.

To implement the prior art techniques, including those suggested by Hughes and Angelo, it is necessary for a service provider to distribute physical 'removable media' to all their on-line clients. This would obviously be expensive, slow and not feasible as a mass market solution for the service providers. It would be uncomfortable for the clients, as well, since they would need a different physical device for each application, for example, a smart card for online mail, one for a book retailer, etc. The prior art suggests no solution to this problem.

According to the method of the present invention, one of the uses of the device is for secure transmission of passwords. Such passwords could be initially communicated to the user through a non-Internet communication channel (phone or post), entered by the user into the secure keyboard and stored inside it in non-volatile memory. From then on, these passwords would be used as access control to on-line services in a perfectly secure manner (since the passwords would only pass through the computer in an encrypted state).

It is not apparent from Angelo how passwords are written into the 'secured memory'. It is not suggested at any point in the patent that these passwords are entered through the secure keyboard. Furthermore, it is in no way suggested that these passwords would be used for any purpose other than access to the user's own PC. No encryption means are suggested there and the secure channel described between the keyboard and 'secured memory' serves only to allow the computer to check if the password that is entered by the user matches the one in the secured memory. According to Angelo, if the result of this check is positive, then the user is issued access rights to his/her own computer.

It is respectfully put forward by Applicant that there is not any

Hon. Commissioner of Patents and Trademarks
BOX PCT
Washington, D.C. 20231

substantial reason to view the combination of references as obvious, since none of them suggest a self-contained, easy-to-install device which is the keyboard itself, modified so as to contain a chip capable of encryption/decryption and data storage, as provided by the invention. To say that such a combination is obvious to try, as the Examiner seems to do, is one thing, but to recognize the above-outlined design advantages is another thing.

Therefore, independent claims 1 and 22 are deemed to be patentable over the prior art, and the dependent claims are likewise deemed patentable being based thereon.

Based on the attached amendments to the claims and the above remarks, Applicant believes that all of the amended claims present patentable subject matter without raising any new issues, and it is respectfully requested that the Examiner issue the International Preliminary Examination Report to reflect this position as early as possible.

Respectfully submitted,

Edward Langer, Pat. Atty.
Attorney for Applicant
Reg. No. 30, 564

CLAIMS:

1. A secure data entry peripheral device configured as a secure keyboard device in a computer system, said secure keyboard device comprising:

means for at least one of entry, collection and reading of data information;

controller means for encoding said data information for presentation to the computer system, and

means associated with said controller for processing said encoded data information by performing thereon at least one operation amongst operations including encryption, decryption, data manipulation and non-volatile storage,

said processed encoded data information providing a secure transaction when transmitted within the computer system, and when decrypted and decoded for use at a remote location,

wherein said controller means is a keyboard encoder and said processing means comprises an electronic device capable of encrypting/decrypting and storing data entered via said keyboard,

wherein said keyboard encoder and said electronic device comprise a single integrated device,

and wherein said single integrated device does not use removable media such as Smartcard, security token and the like.

2. Deleted

3. Deleted

4. Deleted

5. Deleted

6. Deleted

7. Deleted

8. Deleted

9. Deleted

10. Deleted

11. Deleted

12. The device of claim 1 wherein said single integrated device includes an internal EEPROM memory as an integral part of said device, which stores secure information.

13. The device of claim 1 wherein said single integrated device includes secure, protected encryption keys and data as an internal and integral non-removable element.

14. The device of claim 1 wherein said single integrated device further comprises a secure command interpreter which operates to manipulate commands.

15. The device of claim 1 wherein said single integrated device is capable of preventing unauthorized use of software programs.

16. Deleted

17. Deleted

18. Deleted.

19. Deleted

20. Deleted

21. Deleted

22. A method of providing secure data entry in a computer system, said method comprising the steps of:

performing at least one of entry, collection and reading of data information via a standard data entry device configured as a secure keyboard device;

encoding said data information within said standard data entry device for presentation to the computer system, and

processing, within said standard data entry device, said encoded data information by performing thereon at least one operation amongst operations including encryption, decryption, data manipulation and non-volatile storage,

said processed encoded data information providing a secure transaction when transmitted within the computer system, and when decrypted and decoded for use at a remote location,

wherein said encoding step is performed by a keyboard encoder and said processing step is performed by an electronic device capable of encrypting/decrypting and storing data entered via said keyboard,

wherein said keyboard encoder and said electronic device comprise a single integrated device, and

wherein said single integrated device does not use removable media such as a Smartcard, security token and the like.

23. Deleted.

24. Deleted.